Research Proposal: Utilizing Microservices for Healthcare Systems

Jeffrey Leung[1]

[1] *Simon Fraser University*

June 15, 2017

Abstract

This paper is an assignment for CMPT 376W: Technical Writing and Group Dynamics. Recent ransomeware attacks on healthcare systems revealed critical weakpoints in the technological systems used for healthcare. This paper proposes a review on how microservice conventions can be standardized for the use of healthcare systems to provide an opinionated solution which addresses these weakpoints. The objective of this review would be to suggest the adoption of architectures and strategies particularly for such technological systems.

1 Introduction

Out of the essential services declared by the government, healthcare is possibly the most urgent and vital. Societies depend heavily on health services to sustain the physical and mental wellbeing of citizens. As such, it was a great shock to the world when the technical operations of the National Health Service (NHS) of England, Scotland, and Wales were crippled for multiple days from a ransomware attack named WannaCry [1]. This incident served as a terrifying reminder that technological systems utilized for critical operations will always be vulnerable to malicious attack. Few if any standards currently exist for the architecting of systems used for critical medical purposes. Whereas microservices are an increasingly common concept effective for large web server systems, this document proposes a formal review of whether standards inspired by strategies derived from microservice design [2] can be drawn up for the purpose of regulating and improving the technological architecture of systems used for healthcare purposes. The proposed review will define avenues of direct applicability of microservice design approaches for technological healthcare systems.

2 Problem Description

The WannaCry attack on the NHS was an example of ransomware, or malicious software which prevents access to files or to an entire operating system. The ransomware was injected through a vulnerability in an older version of Windows, which many of the compromised servers were running. Though this was only one of the many factors in this incident, the reluctance to upgrade archaic technology has been observed consistently regardless of the purpose of the program because upgrading is not viewed as a rewarding short-term investment.

Healthcare systems need to be highly

available because they often handle critical information and services. This often conflicts with the need to keep a system updated, since changes to a running program will temporarily remove the program from usage. Large archaic systems are relatively unreliable and difficult to start or stop, which potentially leads to lengthier downtime. The attack on the NHS caused several days of downtime, during which many patients' health were severely compromised.

Over the past few years, microservices have been hailed as the silver bullet of the issue of large web servers. Microservice architecture is loosely defined as the disassembly of a single application into small modular services in independent processes [3]. As a solution to many issues stemming from large monolithic programs, breaking up an application into microservices allows for many improvements such as increased scalability, or the ability to increase performance for more durable usage under stress. Whenever an application has replicated functionality, programmers will consider ways to move the functionality to a single, discrete module. Similarly, whenever an application has too much functionality, programmers will attempt to split the functionality into separate applications.

3 Objectives of the Proposed Research

I propose a review on healthcare systems and microservice conventions. In this review, I will:

- research established standards for designing technological healthcare systems if any currently exist,
- determine which microservice design approaches would be best suited for such systems given their nature and needs, and
- suggest adoption of specific architecture strategies as best practices.

Though there are many standards and regulations for healthcare itself, the technological programs which support healthcare are relatively new and the scope of their abilities are continually increasing so there has been little opportunity to research and implement standards. The proposed review will include communication between software architects of many health service providers around the world to understand the nuanced issues which have arisen from the nature of using technology in healthcare. Though the WannaCry incident had the most debilitating impact thus far it is not the only incident which has occurred so it is expected that various other healthcare system designers will have encountered issues.

The microservice architecture has been chosen as the basis of this research for numerous reasons. For example, programmers are often shackled with immense legacy systems which resist change due to the possible impacts potentially caused by small modifications, but microservices allow for a greater ease of change because possible impacts are reduced to a single component on its own server. The component becomes easier to change, upgrade, and deploy, which encourages the addition of many smaller improvements. Upgrading the system to a new framework or operating system and keeping it up to date becomes more feasible, which could alleviate one of the issues of the WannaCry attack. Research will be required to determine whether this would assist in the development process of such a system, based on the nature of software development on similar services.

Large applications have much less flexibility to scale horizontally meaning replication across multiple discrete servers to increase performance, and instead are restricted to scaling vertically meaning upgrades to more powerful servers to increase performance. Scaling horizontally only benefits monolithic

services to a limit due to their size, while microservices benefit greatly due to the smaller scale of each component. Healthcare systems require greater availability as even a minute of downtime could cause casualties. Moving to a microservice design would allow near-infinite scalability and an increase in uptime. Research needs to be conducted to determine the amount of scalability and recovery which is needed by a healthcare system. This research would include the collection of past usage and load data, the forcasting of expected user loads, and the simulation of possible emergency situations.

Services can be placed into more diverse environments by using a microservice design. This is possible since the APIs between microservices are often agnostic of language or technology [4]. For example, a component can be deployed on multiple servers, each running a different operating system such as Red Hat Enterprise Linux, Ubuntu, and Windows. If an operating system vulnerability is exploited such as in the WannaCry incident, not all the servers will be incapacitated. This would be vital in the situation of a zero-day exploit which is a vulnerability exploited while the maintainer is unaware of its existence. By the definition of a zero-day exploit, a user of the system likely has no defense against it which could endanger all programs relying on that system. Deploying services on multiple operating system provides additional guard against this type of exploit. Deploying the servers in different locations also relieves the possibility of physical issues such as earthquakes or electrical problems. In essence, microservices allow for variable distribution as well as compartmentalized fault tolerance. To determine the necessity of this strategy, research into other previous incidents crippling a system is required.

From the research conducted on how microservice architecture could benefit healthcare services, I propose that specific strategies be compiled into a set of guidelines. These guidelines would define best practices in building a system with outstanding modifiability, availability, and fault-tolerance.

4 Significance

It is of vital importance that systems built for healthcare progress towards being as reliable and impenetrable as possible and the WannaCry attack has violently exposed this need. The more vulnerable these systems are, the greater the risk of injuries and casualties. Utilizing a microservice architecture may create many solutions to the vulnerabilities of these systems and provide significant improvements in their underlying design.

References

[1] N. H. S. Digital, "Updated statement on reported nhs cyber-attack (13 may)," May 2017. [Online]. Available: https://digital.nhs.uk/services/data-security-centre/data-security-centre-latest-news/updated-statement-on-reported-nhs-cyber-attack-13-may

[2] T. Q. Thanh, S. Covaci, T. Magedanz, P. Gouvas, and A. Zafeiropoulos, "Embedding security and privacy into the development and operation of cloud applications and services," *2016 17th International Telecommunications Network Strategy and Planning Symposium (Networks)*, pp. 31–36, Sep. 2016. [Online]. Available: http://ieeexplore.ieee.org.proxy.lib.sfu.ca/document/7751149/

[3] J. Lewis and M. Fowler, "Microservices - a definition of this new architectural term," Mar. 2014. [Online]. Available: https://martinfowler.com/articles/microservices.html

[4] D. Linthicum, "Practical use of microservices in moving workloads to the cloud," *IEEE Cloud Computing*, vol. 3, pp. 6–9, Nov. 2016. [Online]. Available: http://ieeexplore.ieee.org.proxy.lib.sfu.ca/document/7742277/